八幡市情報セキュリティポリシー

令和８年３月一部改定版（基本方針のみ）

２００４(平成１６)年　１月１９日策定
２００７(平成１９)年　３月３０日全部改定
２００９(平成２１)年　６月３０日一部改定
２０１４(平成２６)年　９月３０日一部改定
２０１６(平成２８)年　９月２０日一部改定
２０２０(令和　２)年　８月２１日一部改定
２０２１(令和　３)年　８月１２日一部改定
２０２３(令和　５)年　８月２９日一部改定
２０２４(令和　６)年　９月　９日一部改定
２０２６(令和　８)年　３月２３日一部改定（基本方針のみ）

八幡市ＩＴ推進本部

目次

はじめに

セキュリティポリシーの目的

情報を収集し、保有し、又は利用しようとする者には、それぞれが目指すところ、目指す事柄に応じて自らの行動を律し、その実現に努めることが求められる。

この時に拠り所とした内容を総合し、又は集約したものを、制定形式に拘わらず行動規範と呼び、このうち、その者が管理すべき情報の価値を守り、又は当該情報のうち、秘匿すべきものの安全性を確保するために設定する方針、基準その他の措置を「情報セキュリティポリシー」と呼ぶ。

本市の情報管理施策の経過

・平成　元年１２月「八幡市電子計算機の利用に係る個人情報の保護に関する条例」を施行
・平成１１年１０月「八幡市情報公開条例」を施行
・平成１３年　６月「八幡市個人情報保護条例」を施行
・平成１５年　２月「八幡市コンピュータシステムの管理、運用及び情報保護に関する規則（以下「規則」という。）」をはじめとする１２の基準を施行
・平成１６年　１月「八幡市情報セキュリティポリシー」を施行
・平成１９年　３月「八幡市情報セキュリティポリシー」を全部改定
・平成２１年　６月「八幡市情報セキュリティポリシー」を一部改定
・平成２６年　９月「八幡市情報セキュリティポリシー」を一部改定
・平成２８年　９月「八幡市情報セキュリティポリシー」を一部改定
・令和　２年　８月「八幡市情報セキュリティポリシー」を一部改定
・令和　３年　８月「八幡市情報セキュリティポリシー」を一部改定
・令和　５年　８月「八幡市情報セキュリティポリシー」を一部改定
・令和　６年　９月「八幡市情報セキュリティポリシー」を一部改定

情報セキュリティポリシーの構成

八幡市情報セキュリティポリシーは、本市が組織的に管理する情報をどのような理念に基づき、どのように保護し、又は利用するのかについて、現行の法体系及び計画との関係を調整したうえで、総合的かつ体系的に取りまとめたものである。

規定する内容については、情報の資産的価値に着目してその保全を図るだけに留まらず、当該情報の主体（当事者）と密接に関係する様々な権利の保護の実現に資するものでなければならない。

さらに、この実行性を確保するためには、情報処理業務に携わる本市の職員等（規則第２条第１６号に規定する「職員等」をいう。）及び当該処理業務を受託した事業者（以下「受託業者」という。）に情報セキュリティポリシーを普及し、浸透し、及び定着させることが前提となるため、安定的な規範であることが望ましい。

他方、情報通信技術の急速な進歩・革新に伴う環境の変化、プライバシーを取り巻く社会情勢の変化へ柔軟に対応することも重要である。

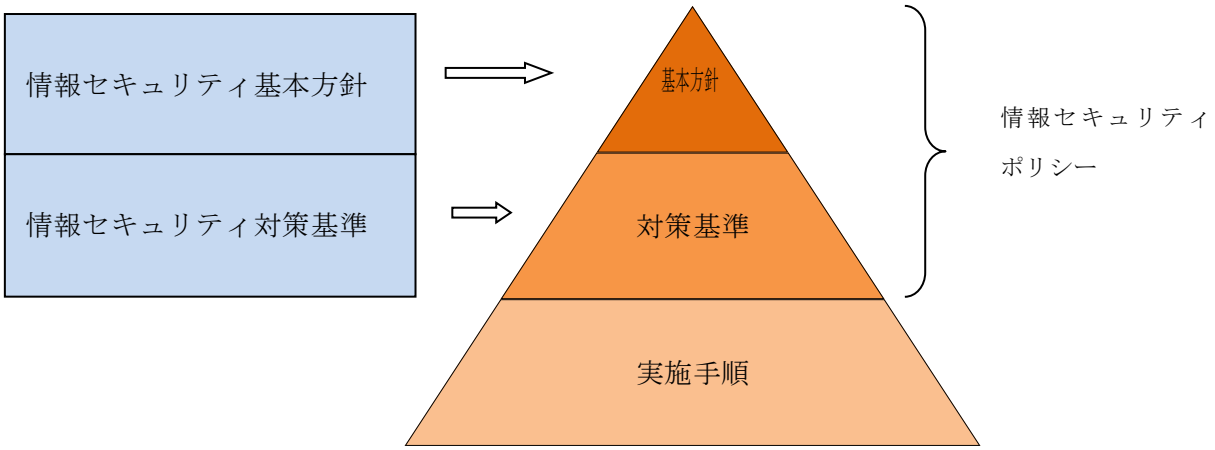
このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と管理客体を取り巻く状況の変化に即応する部分(対策基準)とに分けて策定することとした。

具体的には、情報セキュリティポリシーを「情報セキュリティ基本方針」及び「情報セキュリティ対策基準」２階層で構成することとし、これらに基づき、コンピュータシステムごとの具体的な情報セキュリティ対策の実施手順を示した「情報セキュリティ実施手順」を策定することとした(次頁参照)。本書は情報セキュリティポリシーのうち基本方針のみを収録し、対策基準および実施手順は別に定める。

また、情報セキュリティポリシーに規定した義務、制限の実効性は、強制規範である法令等が、当該法令等の所掌する範囲内において担保すべき事柄であるとの考えから、コンピュータシステムの機能別の遵守事項を規則、規程、基準等として体系化することにより、情報管理施策を総合的に進めることとした。

情報セキュリティポリシーの階層的構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	「情報セキュリティポリシー」全体を統括する理念及び情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	「情報セキュリティ基本方針」を実行に移すために本市が行政全般で利用するネットワーク、コンピュータシステム及びこれらを操作することにより作成され、又は保管される情報資産に関する情報セキュリティ対策の標準
情報セキュリティ実施手順		事案ごとにネットワーク、コンピュータシステム及び情報資産の保護対策を定める「情報セキュリティ対策基準」に基づく具体的な実施手順



第１章　情報セキュリティ基本方針

１．目的

本市が管理し、又は保有するコンピュータシステムが取り扱う情報には、市民等の個人情報、法人等の内部管理情報、行政運営上重要な情報等、外部へ漏えい、又は流出した場合には、極めて重大な事態を招くおそれのある情報が多数含まれており、これら情報資産の機密性、完全性及び可用性を維持する必要がある。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

このため、情報資産並びにそれを取り扱うコンピュータシステム及びネットワークを様々な脅威から防御することは、市民の生命、財産、プライバシー等を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠なものである。

さらに、ICT による行政の推進が積極的に進められる中、本市も ICT を活用し、業務効率化・高度化、住民サービスの向上等を行うためには、全てのネットワーク及びコンピュータシステムにおいて、高度な安全性を確保することは、最優先すべき課題である。

以上のことを踏まえて、本市の保有する情報の機密性、完全性及び可用性を維持するための対策を整備するために「八幡市情報セキュリティポリシー」（以下、「情報セキュリティポリシー」という）を定めるものである。

このうち、「情報セキュリティ基本方針」については、本市が情報セキュリティ対策を講ずるうえで根幹となり、また、展開される施策、実行される対策の是非を判定するための指針となるものであるため、一定の普遍性及び安定性を兼ね備えたものとし、かつ、ICT 関連の専門用語の使用を精査したうえで、情報セキュリティポリシーの位置づけ、対象範囲等について規定することとした。

２．定義

（１）　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）　情報システム（コンピュータシステム）

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（3） 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（4） 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5） 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（6） 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（7） 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（8） マイナンバー利用事務系(個人番号利用事務系)

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（9） LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系(個人番号利用事務系)を除く。）。

(10) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３．情報セキュリティポリシーの策定根拠

本市における情報セキュリティポリシーは、デジタル社会形成基本法第３３条に規定する「サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。第三十七条第二項第十四号において同じ。）の確保、情報通信技術を用いた犯罪の防止、情報通信技術を用いた本人確認の信頼性の確保、情報の改変の防止、高度情報通信ネットワークの災害対策、個人情報の保護その他の国民が安心して高度情報通信ネットワークの利用及び情報通信技術を用いた情報の活用を行うことができるようにするために必要な措置」及び個人情報の保護に関する法律第１２条に規定する「地方公共団体は、その機関が保有する個人情

報の適正な取扱いが確保されるよう必要な措置」の一環として策定する。また、本基本方針は、地方自治法第 244 条の 6 に規定する情報システムの利用に当たってのサイバーセキュリティを確保するための方針として定め、公表するものであり、総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」を踏まえ策定し、必要に応じて見直しを行う。

4．情報セキュリティポリシーの位置づけと職員等及び受託業者の遵守義務

情報セキュリティポリシーは、個人情報の保護に関する法律及び関係条例等、規則をはじめとする情報管理分野の法体系とともに、本市の情報セキュリティ対策における中核をなす非常に重要な規範である。

したがって、本市が保有する情報資産の管理業務又は処理業務に携わるすべての職員等（職員、会計年度任用職員その他本市の業務に従事する者をいう。以下同じ。）及び受託業者は、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たっては、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

5．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（1） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（4） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

6．適用範囲

（1） 行政機関の範囲

本基本方針が適用される行政機関は、市長部局、行政委員会、議会事務局、消防本部及び地方公営企業(水道事業を含む。)とする。

（2） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報(これらを印刷した文書を含む)

③情報システムの仕様書及びネットワーク図等のシステム関連文書

7．情報セキュリティ対策

上記５の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1） 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（2） 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（3） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系(個人番号利用事務系)においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、京都府及び京都府下市町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（4） 物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（5） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（8） 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

クラウドサービスを利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディ

アサービスごとの責任者を定める。

（9） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

8．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

9．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果等に基づき、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要な場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで情報セキュリティポリシーを見直す。

10．情報セキュリティ対策基準の策定

上記７、８及び９に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

11．情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。